UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,115	06/27/2001	Geoffrey Huang	CISCP204	7433

22434	7590	10/21/2004

BEYER WEAVER & THOMAS LLP
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/894,115	HUANG ET AL.
	Examiner	Art Unit
	David G. Cervetti	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*27 June 2001*</u>.

2a)☐ This action is **FINAL.** 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☒ Claim(s) *34 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 June 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they include the following reference characters not mentioned in the

description: Figure 3, Number 308, and Figure 4, Numbers 55, 57, and 59. Corrected

drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification

to add the reference characters in the description in compliance with 37 CFR 1.121(b)

are required in reply to the Office action to avoid abandonment of the application. Any

amended replacement drawing sheet should include all of the figures appearing on the

immediate prior version of the sheet, even if only one figure is being amended. The

replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as

per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the

changes are not accepted by the examiner, the applicant will be notified and informed of

any required corrective action in the next Office action. The objection to the drawings

will not be held in abeyance.

Specification

The abstract of the disclosure is objected to because it exceeds 150 words in

length. Correction is required. See MPEP § 608.01(b).

The attempt to incorporate subject matter into this application by reference to

"Internet Security Association and key management protocol (ISAKMP)" RFC 2408,

"The Internet Key Exchange" RFC 2409, and "Security Architecture for the Internet

Protocol" RFC 2401 is improper because they are considered essential material. An

application for a patent when filed may incorporate "essential material" by reference to

(1) a U.S. patent, (2) a U.S. patent application publication, or (3) a pending U.S.

application, subject to the conditions set forth below. Essential material" is defined as

that which is necessary to (1) describe the claimed invention, (2) provide an enabling

disclosure of the claimed invention, or (3) describe the best mode.

The disclosure is objected to because of the following informalities: "which"

(Page 5, line 3), perhaps "wish" was intended, "HTTP, TCP, FTP" (page 8, line 12),

"ATM, IP, ISDN" (page 10, lines 15-16), "MIPS" (page 11, line 4), "RAM", "ROM" (page

11, line 7), "DSL" (page 11, line 15), "ATM", "HSSI", "POS", "FDDI" (page 11, lines 17-

18), "CD-ROM' (page 12, line 13) while well know in the art, these terms have not been

defined.

The use of the trademark "Windows NT" (page 11, line 2) has been noted in this

application. It should be capitalized wherever it appears and be accompanied by the

generic terminology. Although the use of trademarks is permissible in patent

applications, the proprietary nature of the marks should be respected and every effort

made to prevent their use in any manner which might adversely affect their validity as

trademarks. Appropriate correction is required.

Claim Objections

Claims 34 and 40 are objected to because of the following informalities: the

acronym CPU may render the claim indefinite. Please spell out the acronym.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 6, 7, 12, 13, 14, 19, 24, 25, 26, 31, 32, 33, 34, 39, 40, and 45 are

rejected under 35 U.S.C. 102(b) as being anticipated by Mann, et al.

Regarding claims 1 and 14, Mann, et al. teach a method for generating a control

message to be transmitted from a first network device to a second network device in a

data network, the control message relating to an action to be performed at the second

network device, the method comprising:

- determining a first control message to be generated (column 1, lines 40-42);

- identifying reason information relating to at least one reason for generating

  the first control message (column 1, lines 44-49 and 62-68); and

- generating the first control message, the first control message including said

  reason information (column 1, lines 40-42).

Furthermore, with respect to claim 14, Mann, et al. teach a computer program

product for generating a control message (column 5, lines 16-29).

With respect to claim 6, Mann, et al. teach the method of claim 1 further

comprising transmitting the first control message to the second network device (column

3, lines 36-43) to thereby cause the second network device to implement an appropriate

action in response to the first control message (column 2, lines 61-68).

With respect to claims 7 and 19, Mann, et al. teach a method for communicating between nodes in a data network, the method comprising:

- receiving a first control message from a first node, the control message including reason information relating to at least one reason for the generation of the first control message (column 1, lines 40-53 and 54-56);

- identifying the reason information (column 1, lines 56-58);

- determining an appropriate response to the first control message using at least said reason information (column 1, lines 58-62); and

- implementing said appropriate response (column 1, lines 62-68).

Furthermore, with respect to claim 19, Mann, et al. teach a computer program product for communicating between nodes in a data network (column 5, lines 16-29).

With respect to claim 12, Mann, et al. teach the method of claim 7 further comprising:

- implementing a first response to the first control message if the reason information includes a first reason code (column 2, lines 61-68); and

- implementing a second response to the control message if the reason information includes a second reason code (column 13, lines 1-17 and 53-61, column 15, lines 8-22, figure 6B, number 103, figures 6E and 6F).

With respect to claim 13, Mann, et al. teach the method of claim 7 wherein the control message relates to an action to be performed at a network device receiving the control message (column 2, lines 61-68).

With respect to claim 24, Mann, et al. teach the computer program product of claim 19 further comprising:

- computer code for implementing a first response to the first control message if the reason information includes a first reason code (column 2, lines 61-68); and

- computer code for implementing a second response to the control message if the reason information includes a second reason code (column 13, lines 1-17 and 53-61, figure 6B, number 103).

With respect to claim 25, Mann, et al. teach the computer program product of claim 19 wherein the control message relates to an action to be performed at a network device receiving the control message (column 2, lines 61-68).

With respect to claim 26, Mann, et al. teach a system for communicating between nodes in a data network, the system comprising:

- means for receiving a first control message from a first node, the control message including reason information relating to at least one reason for the generation of the first control message (column 1, lines 40-53 and 54-56);

- means for identifying the reason information (column 1, lines 56-58);

- means for determining an appropriate response to the first control message using at least said reason information (column 1, lines 58-62); and

- means for implementing said appropriate response (column 1, lines 62-68).

With respect to claim 31, Mann, et al. teach the system of claim 26 further comprising means for transmitting the first control message to the second network device (column 3, lines 36-43) to thereby cause the second network device to implement an appropriate action in response to the first control message (column 2, lines 61-68).

With respect to claim 32, Mann, et al. teach the system of claim 26 further comprising:

- means for implementing a first response to the first control message if the reason information includes a first reason code (column 2, lines 61-68); and

- means for implementing a second response to the control message if the reason information includes a second reason code (column 13, lines 1-17 and 53-61, figure 6B, number 103).

With respect to claim 33, Mann, et al. teach the system of claim 26 wherein the control message relates to an action to be performed at a network device receiving the control message (column 2, lines 61-68).

With respect to claim 34, Mann, et al. teach a system for generating a control message to be transmitted to a network device in a data network, the control message relating to an action to be performed at the network device, the system comprising:

- at least one CPU (column 2, lines 34-38);

- memory (column 2, lines 34-38); and

- at least one interface for communicating with the network device (figure 2, number 19);

- the system being configured or designed to determine a first control message to be generated (column 1, lines 40-42);

- the system being further configured or designed to identify reason information relating to at least one reason for generating the first control message (column 1, lines 44-49 and 62-68); and

- the system being further configured or designed to generate the first control message, wherein the first control message includes said reason information (column 1, lines 40-42).

With respect to claim 39, Mann, et al. teach the system of claim 34 being further configured or designed to transmit the first control message to a second network device (column 5, lines 30-37) to thereby cause the second network device to implement an appropriate action in response to the first control message (column 5, lines 37-52).

With respect to claim 40, Mann, et al. teach a system for communicating between nodes in a data network, the system comprising:

- at least one CPU (column 2, lines 34-38);

- memory (column 2, lines 34-38); and

- at least one interface for communicating with at least one network device (figure 2, number 19);

- the system being configured or designed to receive a first control message from a first node, the control message including reason information relating to at least one reason for the generation of the first control message (column 1, lines 54-56);

- the system being further configured or designed to identify the reason information (column 1, lines 56-58);

- the system being further configured or designed to determine an appropriate response to the first control message using at least said reason information (column 1, lines 58-62); and

- the system being further configured or designed to implement said appropriate response (column 1, lines 62-68).

With respect to claim 45, Mann, et al. teach the system of claim 40 further comprising:

- the system being further configured or designed to implement a first response to the first control message if the reason information includes a first reason code (column 2, lines 61-68); and

- the system being further configured or designed to implement a second response to the control message if the reason information includes a second reason code (column 13, lines 1-17 and 53-61, figure 6B, number 103).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 3, and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mann, et al. as applied to claim 1 above, and further in view of Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 1 above. However, Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE), the Security Architecture for the Internet Protocol (IP Security), or the Internet Security Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet Security Association and Key Management Protocol (RFC 2408) (page 5, column 2, paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use these three protocols to send messages between nodes in a communications network.

The suggestion/motivation for doing so would have been to protect the messages from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al.

for the benefit of sending messages between nodes in a communications network to

obtain the invention as specified in claims 2, 3, and 4.

Claims 8, 9, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Mann, et al. as applied to claim 7 above, and further in view of Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 7 above. However,

Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE),

the Security Architecture for the Internet Protocol (IP Security), or the Internet Security

Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec

protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet

Security Association and Key Management Protocol (RFC 2408) (page 5, column 2,

paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same

field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary

skill in the art to use these three protocols to send messages between nodes in a

communications network.

The suggestion/motivation for doing so would have been to protect the messages

from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al. for the benefit of sending messages between nodes in a communications network to obtain the invention as specified in claims 8, 9, and 10.

Claims 15, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mann, et al. as applied to claim 14 above, and further in view of Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 14 above. However, Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE), the Security Architecture for the Internet Protocol (IP Security), or the Internet Security Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet Security Association and Key Management Protocol (RFC 2408) (page 5, column 2, paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use these three protocols to send messages between nodes in a communications network.

The suggestion/motivation for doing so would have been to protect the messages from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al.

for the benefit of sending messages between nodes in a communications network to

obtain the invention as specified in claims 15, 16, and 17.

Claims 20, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Mann, et al. as applied to claim 19 above, and further in view of Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 19 above. However,

Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE),

the Security Architecture for the Internet Protocol (IP Security), or the Internet Security

Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec

protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet

Security Association and Key Management Protocol (RFC 2408) (page 5, column 2,

paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same

field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary

skill in the art to use these three protocols to send messages between nodes in a

communications network.

The suggestion/motivation for doing so would have been to protect the messages

from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al.

for the benefit of sending messages between nodes in a communications network to

obtain the invention as specified in claims 21, 21, and 22.

Claims 27, 28, and 29 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Mann, et al. as applied to claim 26 above, and further in view of .

Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 26 above. However,

Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE),

the Security Architecture for the Internet Protocol (IP Security), or the Internet Security

Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec

protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet

Security Association and Key Management Protocol (RFC 2408) (page 5, column 2,

paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same

field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary

skill in the art to use these three protocols to send messages between nodes in a

communications network.

The suggestion/motivation for doing so would have been to protect the messages

from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al.
for the benefit of sending messages between nodes in a communications network to
obtain the invention as specified in claims 27, 28, and 29.

Claims 35, 36, and 37 are rejected under 35 U.S.C. 103(a) as being
unpatentable over Mann, et al. as applied to claim 34 above, and further in view of
Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 34 above. However,
Mann, et al. do not disclose expressly that the Internet Key Exchange Protocol (IKE),
the Security Architecture for the Internet Protocol (IP Security), or the Internet Security
Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec
protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet
Security Association and Key Management Protocol (RFC 2408) (page 5, column 2,
paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same
field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary
skill in the art to use these three protocols to send messages between nodes in a
communications network.

The suggestion/motivation for doing so would have been to protect the messages
from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al.

for the benefit of sending messages between nodes in a communications network to

obtain the invention as specified in claims 35, 36, and 37.

Claims 41, 42, and 43 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Mann, et al. as applied to claim 40 above, and further in view of

Troxel, et al.

Mann, et al. teach the limitations as set forth under claim 40 above. However,

Mann, et al. does not disclose expressly that the Internet Key Exchange Protocol (IKE),

the Security Architecture for the Internet Protocol (IP Security), or the Internet Security

Association and Key Management Protocol (ISAKMP) may be used.

Troxel, et al. teach sending messages between nodes in a network using IPSec

protocols (RFC 2401), Internet Key Exchange Protocol (RFC 2409), and Internet

Security Association and Key Management Protocol (RFC 2408) (page 5, column 2,

paragraph 0070).

Mann, et al. and Troxel, et al. are analogous art because they are from the same

field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary

skill in the art to use these three protocols to send messages between nodes in a

communications network.

The suggestion/motivation for doing so would have been to protect the messages

from spoofing attacks.

Therefore, it would have been obvious to combine Mann, et al. and Troxel, et al. for the benefit of sending messages between nodes in a communications network to obtain the invention as specified in claims 41, 42, and 43.

Claims 5, 11, 18, 23, 30, 38, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mann, et al. as applied to claims 1, 7, 14, 19, 26, 34, and 40 above respectively, and further in view of Leung.

Mann, et al. teach the limitations as set forth under claims 1, 7, 14, 19, 26, 34, and 40 above. However, Mann, et al. do not disclose expressly that the message may be used to modify a security association.

Leung teaches using packets (messages) for configuration, modification, and retrieval of security associations (column 5, lines 5-15 and 30-35).

Mann, et al. and Leung are analogous art because they are from the same field of endeavor, sending messages between nodes in a communications network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to send messages between nodes in a communications network to modify a security association.

The suggestion/motivation for doing so would have been to reduce the administrative support required to configure and modify the security associations.

Therefore, it would have been obvious to combine Mann, et al. and Leung for the benefit of modifying security associations in a communications network to obtain the invention as specified in claim 5, 11, 18, 23, 30, 38, and 44.

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. US Patent Number 6418205, filed May 7, 1998, inventors:

Capers et al. Title: Call and circuit state machine for a transaction control layer of a

communications signaling gateway.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to David G. Cervetti whose telephone number is n/a. The

examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on (703) 305-9648. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100